I Settimana (20 - 22 febbraio 2012)

Introduzione al corso. Richiami sulla divisibilità in $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[i]$. Richiami sulle proprietà delle congruenze in $\mathbb{Z}$. Richiami sulle proprietà dell'anello $\mathbb{Z}/n\mathbb{Z}$ e del gruppo moltiplicativo dei suoi elementi invertibili. Sistemi completi di residui (mod n). Inverso aritmetico (mod n). Sistemi ridotti di residui (mod n). Equazioni diofantee e congruenze polinomiali. Teorema fondamentale sulla risolubilità delle congruenze del tipo $aX \equiv b \pmod{n}$. Esempi.

II Settimana (27 - 29 febbraio 2012)

Congruenze lineari ed equazioni diofantee lineari del tipo $aX + cY = b$.
Il Teorema cinese dei resti.
Criteri di divisibilità per 2, 3, 4, 5, 9, 11, 2^m, 5^m, 1001.
Il Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson.
Il piccolo Teorema di Fermat. Teorema di Eulero-Fermat. Numeri pseudo-primi.

III Settimana (5 - 7 marzo 2012)

Esistenza di infiniti numeri primi. Esistenza di infiniti numeri primi del tipo $4k + 3$.
Studio della congruenza $X^2 \equiv -1 \pmod{p}$. Applicazioni del piccolo teorema di Eulero-Fermat e del teorema di Wilson. Esponenziazione modulare. Esempi ed esercizi.
Risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{n}$. Riconduzione del problema generale al caso della risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{p^n}$ con p numero primo. Esempi.
Procedimento di determinazione delle soluzioni di $f(X) \equiv 0 \pmod{p^{n+1}}$ a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p^n}$. Esempi.

IV Settimana (12 - 14 marzo 2012)

Polinomi di $\mathbb{Z}[X]$ identicamente congrui (mod n); polinomi di $\mathbb{Z}[X]$ equivalenti (mod n). Congruenze polinomiali (mod p), con p numero primo.
Congruenza del tipo $X^{p-1} - 1 \equiv 0 \pmod{p^n}$, con p numero primo.
Congruenze del tipo $X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ e $X^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ con p numero primo dispari.
Congruenza del tipo $X^{\frac{p(p-1)}{2}} - 1 \equiv 0 \pmod{p^2}$, con p numero primo dispari. Esempi.
Esistenza di infiniti numeri primi p per i quali la congruenza $f(X) \equiv 0 \pmod{p}$ è risolubile. Esistenza di infiniti numeri primi del tipo $4k + 1$.
Teorema di Lagrange.

V Settimana (19 - 21 marzo 2012)

Il gruppo U_n. Ordine di un intero modulo n.
Radici primitive modulo n.

Un gruppo abeliano finito ha un elemento di ordine l'esponente del gruppo. Un sottogruppo finito del gruppo moltiplicativo di un campo è ciclico. U_p con p numero primo è ciclico. U_{p^e} con p numero primo dispari ed $e \geqslant 1$ è ciclico. Dimostrazione del teorema di Gauss sull'esistenza di radici primitive.

VI Settimana (26 - 28 marzo 2012)

Radici primitive ed indici. Proprietà degli indici. Tabelle degli indici.
Congruenze del tipo $X^m \equiv a \pmod{n}$ con n che possiede una radice primitiva. Criterio di risolubulità di Gauss .
Congruenze del tipo $X^m \equiv a \pmod{p}$ con p primo. Criterio di risolubulità di Eulero.
Risolubilità delle congruenze esponenziali del tipo $a^X \equiv b \pmod{p}$. Esempi ed esercizi.

VII Settimana (16 - 18 aprile 2009)

Congruenze quadratiche e riduzione al caso $X^2 \equiv a \pmod{n}$. Residui quadratici di n. Il gruppo Q_n dei residui quadratici di n. Se $n = 2,\ 4,\ p^h,\ 2p^h$ con p primo dispari, allora Q_n è un gruppo ciclico con $\varphi(n)/2$ elementi . Simbolo di Legendre e sue proprietà. Lemma di Gauss per il calcolo del simbolo di Legendre. Calcolo di $\left(\frac{2}{p}\right)$ con il lemma di Gauss. Definizione di $\sigma_{a,p}$ e dimostrazione della sua relazione con il simbolo di Legendre. LRQ

VIII Settimana (23 - 27 aprile)

Richiami sugli argomenti della settimana precedente. LRQ e suoi corollari. Algoritmo per il calcolo del simbolo di Legendre. Esempi. Calcolo di $\left(\frac{3}{p}\right)$ con la LRQ. Congruenze quadratiche del tipo $X^2 \equiv a \pmod{p^e}$. Congruenze quadratiche del tipo $X^2 \equiv a \pmod{2^e}$. Numero delle soluzioni incongruenti di congruenze quadratiche del tipo $X^2 \equiv 1 \pmod{2^e}$. Numero delle soluzioni incongruenti di congruenze quadratiche del tipo $X^2 \equiv a \pmod{2^e}$.

IX Settimana (2 - 4 maggio)

Numero delle soluzioni incongruenti di congruenze quadratiche del tipo $X^2 \equiv a \pmod{n}$. Simbolo di Jacobi ed estensione della LRQ.
Terne pitagoriche. Esempi. Esercizi. Non esistono triangoli pitagorici isosceli. Le equazioni diofantee $X^4 + Y^4 = Z^2$ e $X^4 + Y^4 = Z^4$.

X Settimana (7 - 9 maggio)

Cenni sull'Ultimo Teorema di Fermat e sull'anello di Kummer delle radici p-esime dell'unità.

S_k. Numeri primi esprimibili come somma di due quadrati. Numeri interi somma di due quadrati. Esempi. Identità di Eulero. Cenni sui quaternioni di Hamilton.

XI Settimana (14 - 16 - 19 maggio)

Per ogni primo dispari p la congruenza $X^2 + Y^2 \equiv -1 \pmod{p}$ ha soluzioni (due dimostrazioni). Ogni intero positivo si può scrivere come somma di quattro quadrati di interi. Numeri interi somma di tre quadrati.
Richiami sui campi $\mathbb{Q}[\sqrt{d}]$ e sugli anelli $\mathbb{Z}[\sqrt{d}]$. Equazione di Pell. Dimostrazione dell'esistenza di una soluzione (x, y) con $x > 0$ e $y > 0$ dell'equazione di Pell. Dimostrazione dell'esistenza di infinite soluzioni dell'equazione di Pell.

XII Settimana (21 maggio)

Frazioni continuate finite semplici e numeri razionali. Cenni sulle frazioni continuate semplici. Risolubilità dell'equazione diofantea $aX + bY = c$ tramite le funzioni continuate finite semplici. Esercizi.